BAB I
PENDAHULUAN

1.1. Latar Belakang

Dalam pengembangan teknologi yang sangat pesat saat ini. Teknologi dalam komputer sudah menjadi sangat menjadi bidang pengembangan yang sangat pesat. Dalam hal ini ialah dibutuhkannya keamanan data ketika mengirimkan suatu permintaan pada pembelian barang, dalam hal tiket misalnya. Siapapun dapat bisa membeli tiket dengan mudahnya, salah satu contohnya ialah tiket transportasi udara yang dapat dipesan melalui sistem *online* melalui situs jaringan internet ataupun aplikasi.

Kriptografi (*cryptography*) berasal dari Bahasa Yunani: "*cryptos*" artinya "*secret*" (rahasia), sedangkan "*graphein*" artinya "*writing*" (tulisan). Jadi kriptografi berarti "*secret writing*" (tulisan rahasia). Jadi dapat disimpulkan Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi [6].

Terdapat berbagai macam metode kriptografi yang dibuat kemudian dikemukakan oleh ilmuwan-ilmuwan hingga saat ini. Beberapa kriptografi yang telah diciptakan ialah, *Symmetric-Key Enciphermen* dan *Asymmetric-Key Enciphermen*. *Symmentric-Key Enciphermen* menggunakan single *secret key* untuk kedua enkripsi dan dekripsi. Sedangkan *Asymmetric-Key Enciphermen* menggunakan satu *public key* dan satu *privat key*. Adapun jenis-jenis algoritma untuk *Symmetric-Key* ialah stream cipher, DES, AES, A5/1, dan lain-lain. Sedangkan *Asymmetric-Key* ialah RSA, ECC, ELGAMAL, dan lain-lain[4].

Fungsi *Hash* kriptografi adalah fungsi hash yang memiliki beberapa sifat keamanan tambahan sehingga dapat dipakai untuk tujuan keamanan data.. SHA atau *Security Hash Algorithm* adalah Serangkaian fungsi cryptographic hash yang dirancang oleh National Security Agency (NSA) dan diterbitkan oleh NIST sebagai

US Federal Information Processing Standart. Jenis-jenis SHA yaitu SHA-1 dan SHA-2 yang terbagi menjadi SHA-224, SHA-256, SHA-384 dan SHA-512[4].

1.2. Rumusan Masalah

Rumusan masalah pada pembuatan Proposal Tugas Akhir ini, yaitu:

1. Mengetahui tingkat keamanan dari sistem pembelian tiket *online*
2. Mengetahui kelemahan dari sistem pembelian tiket *online*
3. Menggunakan ECC untuk transaksi pada pembelian tiket online
4. Menggunakan SHA-256 untuk otentikasi data pada pembelian tiket

1.3. Tujuan

Berdasarkan rumusan masalah yang ada, tujuan yang akan dibahas dalam proposal tugas akhir ialah :

a. Melakukan implementasi *Elliptic Curve Cryptography* dengan menggunakan *Security Hash Algorithm 256* sebagai fungsi enkripsi pada sistem pembelian tiket online.
b. Menganalisa proses enkripsi dan dekripsi yang dirancang.
c. Menganalisa proses yang dilakukan untuk pengontetikasi data.

1.4. Batasan Masalah

Adapun batasan masalah pada tugas akhir ini ialah

a. Enkripsi dengan *Elliptic Curve Cryptography* sebagai public key.
b. Fungsi *Secure Hash Algorithm 256* sebagai *Digital Signature*.
c. Proses pembelian dilakukan dilakukan tanpa mendaftarkan akun.

1.5. Hipotesa

ECC menawarkan keamanan yang sebanding dengan RSA dengan kunci yang lebih kecil sehingga mengurangi komputasi[4]. Akan tetapi ECC memiliki kendala dalam proses autentikasi Client yaitu lemahnya sistem autentikasi,Maka dengan digunakannya fungsi Hash tersebut inilah berupaya ada kemungkinan ECC akan

menggunakan kekuatan secara lebih efisien daripada RSA dan dengan kunci yang terpendek[7].

Diharapkannya dengan menggunakan ECC dengan fungsi hash SHA-256 ini dapat mengamankan proses dalam otentikasi data yang dikirimkan client kepada sistem.

1.6. Metode Penyelesaian

1. **Studi Literature**

   Studi Literatur dilakukan untuk mempelajari hal-hal yang dibutuhkan untuk perancangan sistem. Sumbernya dari berbagai macam yaitu : Buku, Situs Jurnal Online, Situs Buku Online, maupun Jurnal cetak serta teori-teori pendukung dari Situs Pengembangan resmi yang berkaitan dengan Kriptosistem Kurva Elliptik (ECC) dan Fungsi Hash SHA-256 yang dijadikan bahan dalam pembuatan dasar teori dalam pembuatan Tugas Akhir ini.

2. **Analisa**

   Menganalisa masalah-masalah yang terdapat permasalahan yang sedang diteliti dan mendefinisikan batasan masalah yang digunakan untuk memecahkan solusi yang tepat. Hal ini juga termasuk dalam untuk menganalisa keperluan untuk sistem yang akan dirancang.

3. **Perancangan Sistem**

   Ada pun perancangan sistem ini difokuskan pada proses keamanan data yang dikirimkan dengan menggunakan ECC dan SHA-256. Berupa Enkripsi, Dekripsi dan Signature.

4. **Pembuatan Program**

   Pada tahap ini dilakukannya pembuatan program untuk pengujian Enkripsi, Dekripsi dan Signature yang telah dibuat.

5. **Diskusi Ilmiah**

   Adapun perlu dilakukanny diskusi dengan Dosen Pembimbing, narasumber dan lain-lain.